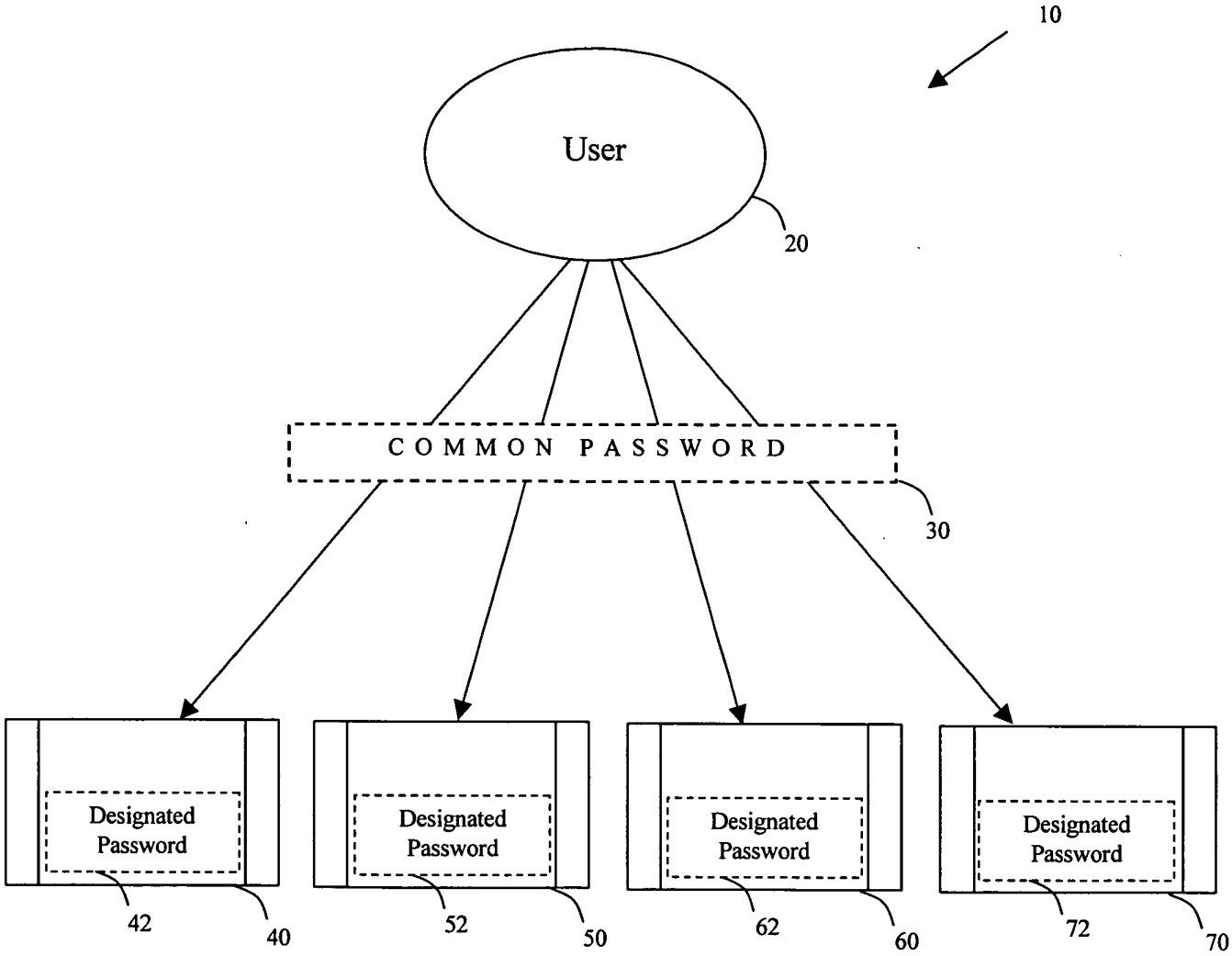

10
User
20
COMMON PASSWORD
30
Designated Password
42
40
Designated Password
52
50
Designated Password
62
60
Designated Password
72
70

FIG. 1

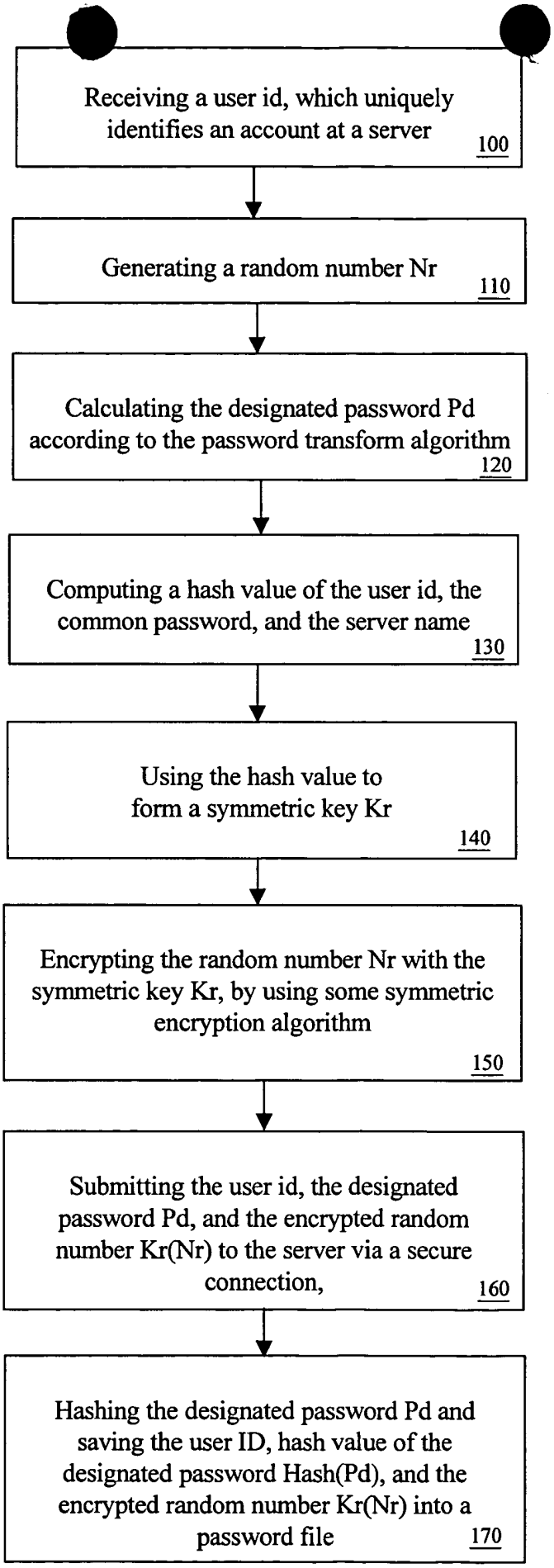

Receiving a user id, which uniquely identifies an account at a server
100
Generating a random number Nr
110
Calculating the designated password Pd according to the password transform algorithm
120
Computing a hash value of the user id, the common password, and the server name
130
Using the hash value to form a symmetric key Kr
140
Encrypting the random number Nr with the symmetric key Kr, by using some symmetric encryption algorithm
150
Submitting the user id, the designated password Pd, and the encrypted random number Kr(Nr) to the server via a secure connection,
160
Hashing the designated password Pd and saving the user ID, hash value of the designated password Hash(Pd), and the encrypted random number Kr(Nr) into a password file
170

FIG. 2

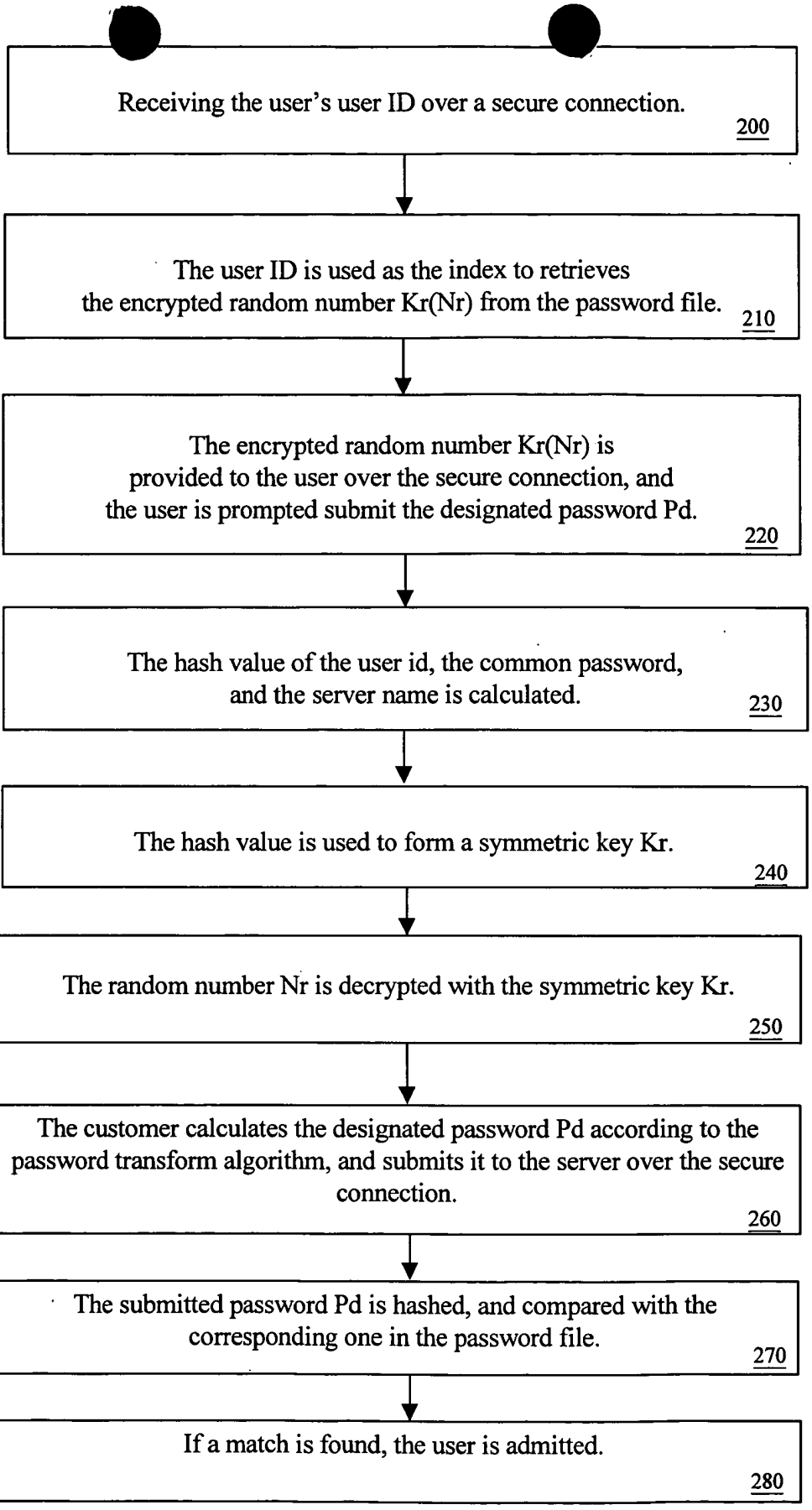

Receiving the user's user ID over a secure connection.
200
The user ID is used as the index to retrieves the encrypted random number Kr(Nr) from the password file.
210
The encrypted random number Kr(Nr) is provided to the user over the secure connection, and the user is prompted submit the designated password Pd.
220
The hash value of the user id, the common password, and the server name is calculated.
230
The hash value is used to form a symmetric key Kr.
240
The random number Nr is decrypted with the symmetric key Kr.
250
The customer calculates the designated password Pd according to the password transform algorithm, and submits it to the server over the secure connection.
260
The submitted password Pd is hashed, and compared with the corresponding one in the password file.
270
If a match is found, the user is admitted.
280

FIG. 3

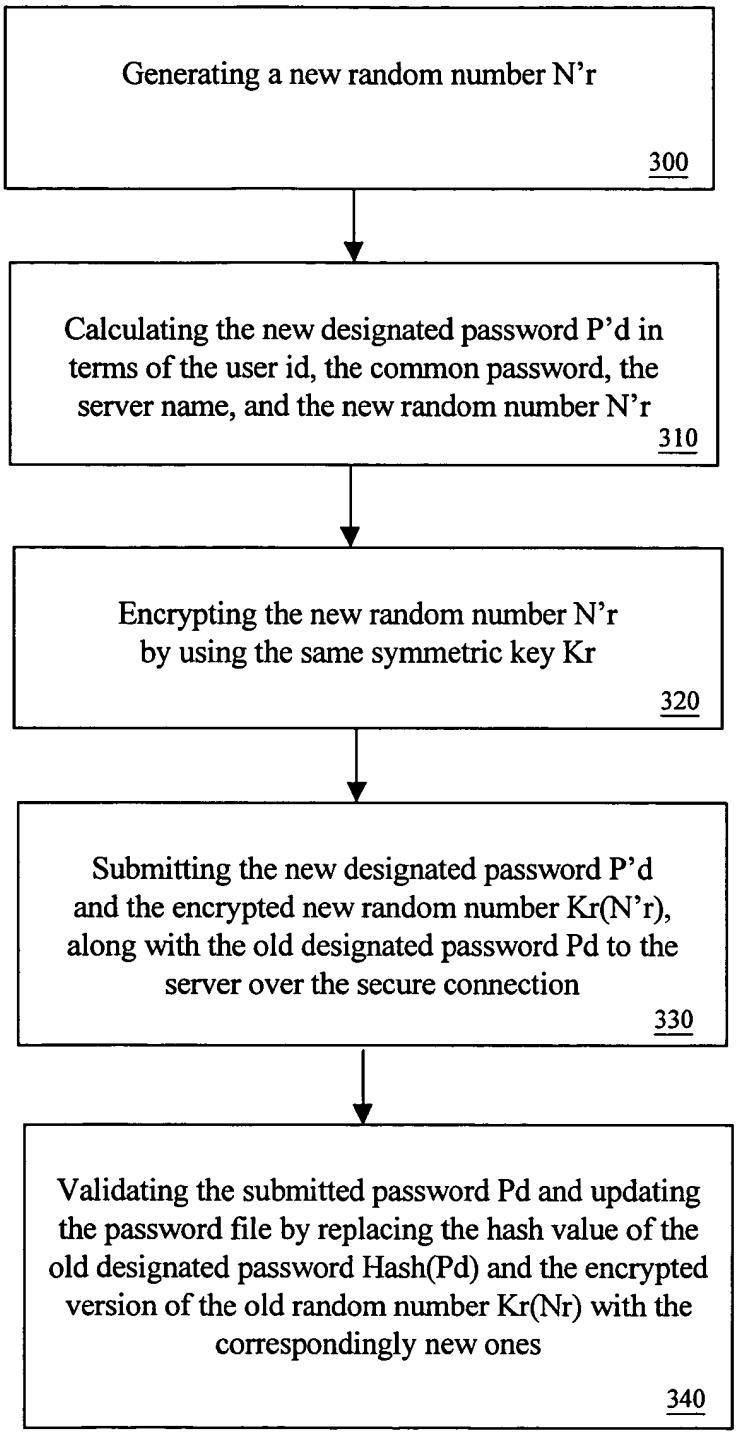
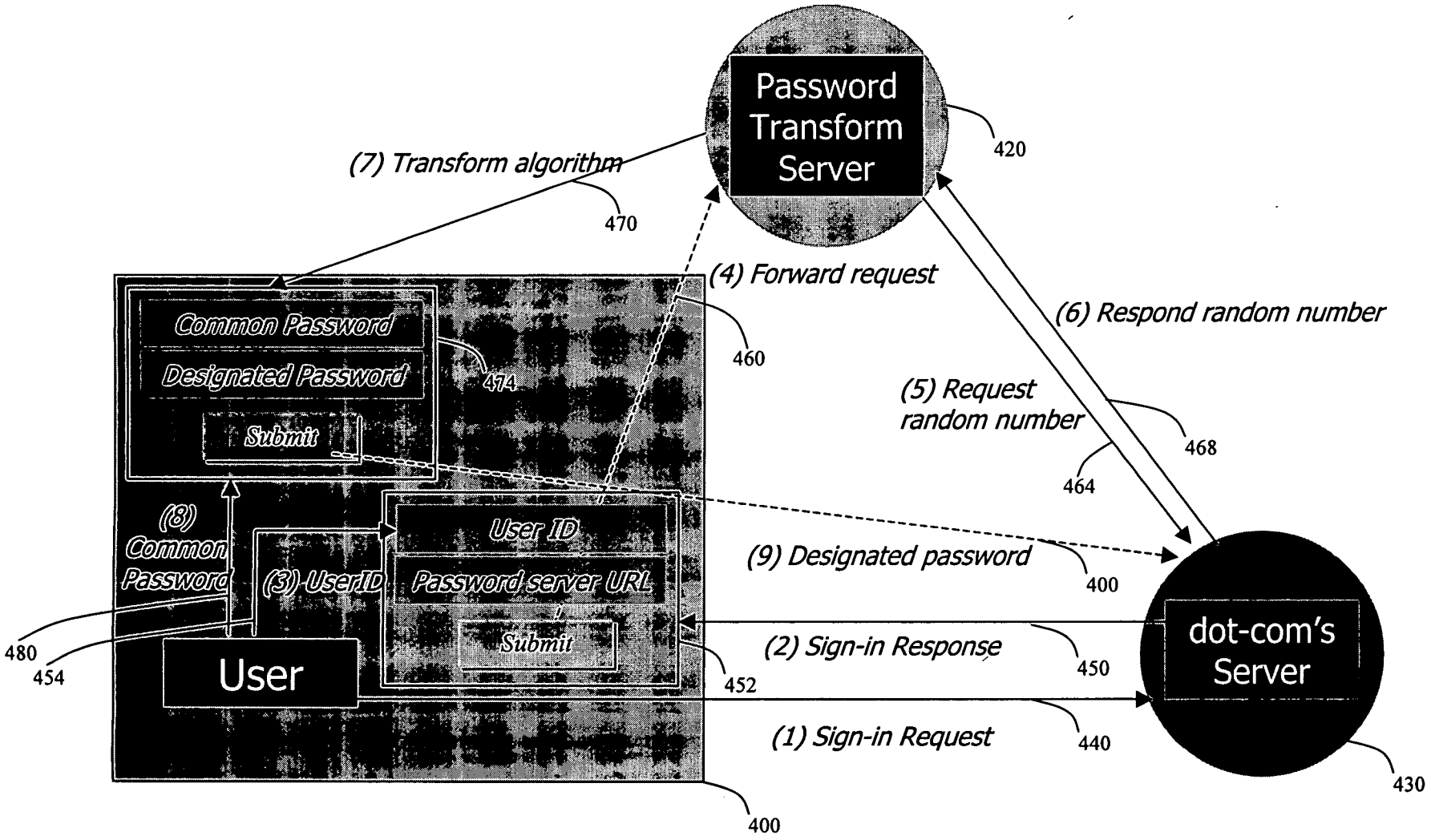

Generating a new random number N'r
300
Calculating the new designated password P'd in terms of the user id, the common password, the server name, and the new random number N'r
310
Encrypting the new random number N'r by using the same symmetric key Kr
320
Submitting the new designated password P'd and the encrypted new random number Kr(N'r), along with the old designated password Pd to the server over the secure connection
330
Validating the submitted password Pd and updating the password file by replacing the hash value of the old designated password Hash(Pd) and the encrypted version of the old random number Kr(Nr) with the correspondingly new ones
340

FIG. 4



Best Available Copy

FIG. 5

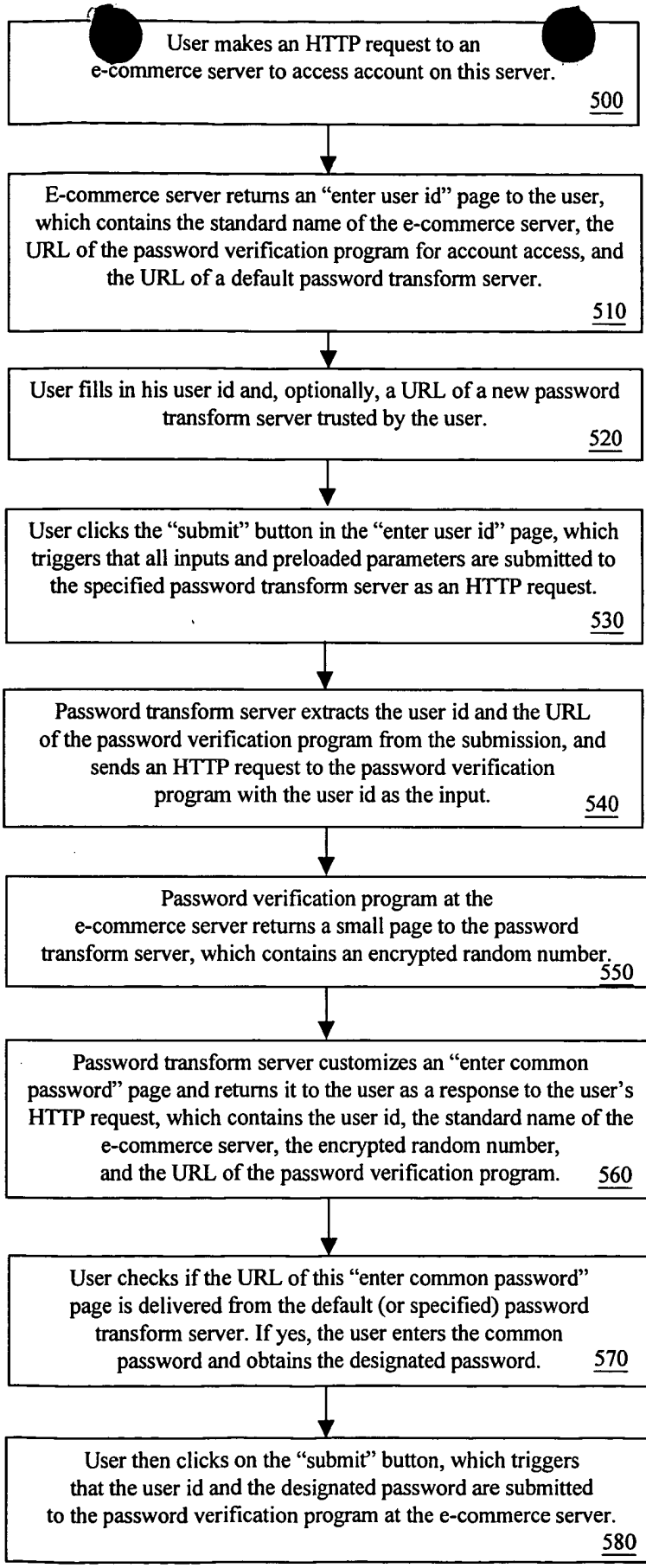

User makes an HTTP request to an e-commerce server to access account on this server. 500
E-commerce server returns an "enter user id" page to the user, which contains the standard name of the e-commerce server, the URL of the password verification program for account access, and the URL of a default password transform server. 510
User fills in his user id and, optionally, a URL of a new password transform server trusted by the user. 520
User clicks the "submit" button in the "enter user id" page, which triggers that all inputs and preloaded parameters are submitted to the specified password transform server as an HTTP request. 530
Password transform server extracts the user id and the URL of the password verification program from the submission, and sends an HTTP request to the password verification program with the user id as the input. 540
Password verification program at the e-commerce server returns a small page to the password transform server, which contains an encrypted random number. 550
Password transform server customizes an "enter common password" page and returns it to the user as a response to the user's HTTP request, which contains the user id, the standard name of the e-commerce server, the encrypted random number, and the URL of the password verification program. 560
User checks if the URL of this "enter common password" page is delivered from the default (or specified) password transform server. If yes, the user enters the common password and obtains the designated password. 570
User then clicks on the "submit" button, which triggers that the user id and the designated password are submitted to the password verification program at the e-commerce server. 580

FIG. 6

600

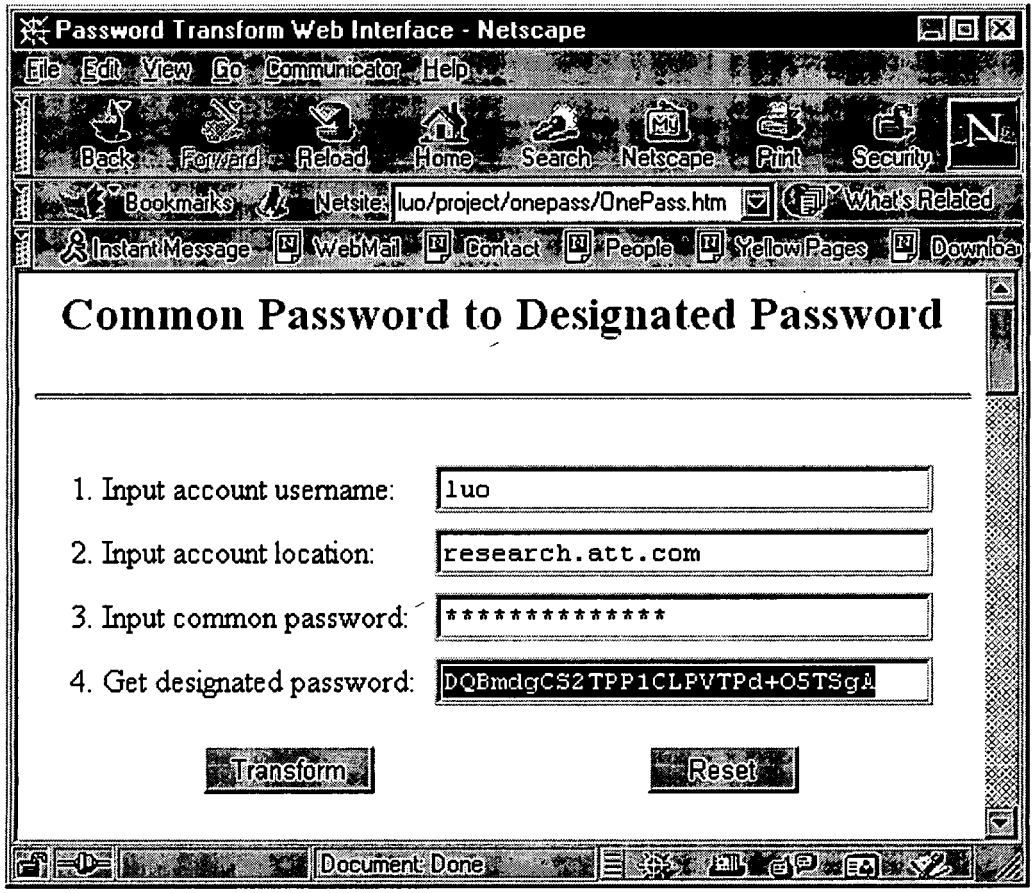


FIG. 7